This paper is being provided in response to the June 28, 2005 Office Action for the above-referenced application. In this response, Applicant has amended Claims 1, 22, 26, 36, 39, and 47, and added new Claims 51-54 in order to clarify that which Applicant deems to be the claimed invention. Applicant respectfully submits that the amendments to the claims and all newly added claims are supported by the originally filed application.

In response to the objection to the drawings as being informal, Applicant respectfully submits that formal drawings will be submitted when a Notice of Allowance is received in connection with this application.

The rejection of Claims 1-8, 13-16, 18-20, 22, 26-30, 36, 39-47, 49 and 50, under 35 U.S.C. § 103(a) as being unpatentable over Wells (U.S. Patent No. 6,338,141, hereinafter referred to as "Wells") in view of Frisch Essential System Administration (hereinafter referred to as "Frisch) and Kim "The Design and Implementation of Tripwire: A File System Integrity Checker" (hereinafter "Kim"). Applicant respectfully submits that the claims, as amended herein, are patentable over the cited art, taken separately or in combination.

Claim 1, as amended herein, recites a method of detecting computer viruses, comprising: providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; an antivirus unit, that uses a particular operating system, scanning at least part of the disk space for viruses,

wherein the part of the disk space that is scanned by the antivirus unit includes at least some

parts of the first and second segments; and the antivirus unit accessing non-native files created

using operating systems different from the particular operating system that is used by the

antivirus unit in connection with scanning at least parts of the disk space for viruses, wherein

said antivirus unit accesses at least one of the segments without using file-based information of

the particular operating system or of any host having access to said at least one segment. Claims

2-8, 13-16 and 18-20 depend from Claim 1.

Claim 22, as amended herein, recites a method of scanning a storage device for viruses,

comprising: performing a first virus scan at a first time; and performing a second virus scan at a

second time after the first time, wherein for said second virus scan, logical entities having a date

of last modification that is after the first time are examined and wherein performing said first and

second virus scans includes using a particular operating system and accessing non-native files

created using operating systems different from the particular operating system, wherein, when

performing a virus scan accessing at least one part of the storage device that is also accessible to

at least one host, said accessing of said at least one part is performed without using file-based

information of the particular operating system or of any host having access to said at least one

part.

Claim 26, as amended herein, recites a computer program product for detecting computer

viruses, comprising: means for accessing a disk space having at least a portion that is partitioned

into separate segments, each segment being accessed by at least one of a plurality of hosts,

wherein a first one of the segments is accessed using a different file system than a second one of

the segments; means that uses a particular operating system for scanning at least part of the disk space for viruses, wherein the part of the disk space that is scanned includes at least some parts of the first and second segments; and means for accessing non-native files created using operating systems different from the particular operating system that is used in connection with scanning at least parts of the disk space for viruses, wherein, when performing a virus scan accessing at least one of the segments that is also accessible to at least one of said plurality of hosts, said accessing of said at least one segment is performed without using file-based information of the particular operating system or of any host having access to said at least one segment. Claims 27-30 depend from Claim 26.

Claim 36, as amended herein, recites a computer program product for scanning a storage device for viruses, comprising: means for performing a first virus scan at a first time; and means for performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system, wherein, when performing a virus scan accessing at least one part of the storage device that is also accessible to at least one host, said accessing of said at least one part is performed without using file-based information of the particular operating system or of any host having access to said at least one part.

Claim 39, as amended herein, recites an antivirus scanning unit, comprising: means for coupling to at least one storage device having at least a portion that is partitioned into separate

segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; means for using a particular operating system for scanning at least part of the at least one storage device for viruses, wherein the part that is scanned includes at least some parts of the first and second segments; and means for accessing non-native files created using operating systems different from the particular operating system that is used in connection with scanning at least parts of the disk space for viruses, wherein, when performing a virus scan accessing at least one of the segments that is also accessible to at least one of said plurality of hosts, said accessing of the at least one segment is performed without using file-based information of the particular operating system or of any host having access to said at least one segment. Claims 40-42 and 44-46 depend from Claim 39.

Claim 47, as amended herein, recites an antivirus unit, comprising: means for performing a first virus scan at a first time; and means for performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system, wherein, when performing a virus scan accessing at least one part of the storage device that is also accessible to at least one host, said accessing of said at least one part is performed without using file-based information of the particular operating system or of any host having access to said at least one part. Claims 49-50 depend from Claim 47.

EMS-00201(2004734-0001)

Wells relates to a stand-alone computer process that uses a single information engine to produce a collection of relational data to detect computer viruses in computer files. The entire process is performed on a single, stand-alone computer system in real time. The process can also be run on the stand-alone system from a connected, remote computer system, which remote system can maintain the known virus databases. (See Abstract; Col. 1, Lines 5-20). Wells discloses a system called Raven as part of a virus detection tool. Raven is run on a given system and the gathered data for each file checked is tested against the relational data that represents the known viruses stored in a virus-detection database. An exact match of all related data indicates a known virus is present. In addition, if most, but not all, of the data is matched, there is a high probability that an unknown (but closely related) virus is present. (Col. 2, Lines 54-62; Figure 5). Page 5 of the Office Action states that Wells does not expressly disclose providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments.

As set forth on page 5 of the Office Action, Frisch teaches a UNIX operating system that enables a flexible partitioning capability wherein each partitioned segment is accessed using a different file system. The Office Action also states on page 5 that Frisch discloses exporting local filesystems by a particular system for network access by other hosts to mount their system.

Page 6 of the Office Action cites Kim as teaching to selectively check the integrity of separate file systems on a disk using the UNIX tool tripwire.

Applicant's Claim 1, as amended herein, is not disclosed or suggested by the references, taken separately or in combination, in that the references do not disclose or suggest *a method of detecting computer viruses, comprising: providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; ... wherein said antivirus unit accesses at least one of the segments without using file-based information of the particular operating system or of any host having access to said at least one segment,* as set forth in Claim 1. Wells discloses detecting viruses by comparing data about a file to relational signature objects created from viruses. Wells' virus scanning is performed on a file-by-file basis and thus must use some file-based information. However, Wells appears silent regarding any further mention about the file-based information used in virus scanning. Frisch discloses dividing a disk into partitions each holding its own file system but fails to make any mention regarding what information is used in connection with accessing a segment during virus scanning. Kim operates on files and appears to use some file-based information. However, Kim appears silent regarding any further mention about the file-based information used in virus scanning.

Based on Applicant's understanding, Page 4 of the Office Action states that the prior art combination of Wells, Frisch and Kim teaches *wherein said antivirus unit accesses at least one of the segments without using file-based information ... of any host having access to said at*

Page 18 of 23

Page 6 of the Office Action cites Kim as teaching to selectively check the integrity of separate file systems on a disk using the UNIX tool tripwire.

Applicant's Claim 1, as amended herein, is not disclosed or suggested by the references, taken separately or in combination, in that the references do not disclose or suggest *a method of detecting computer viruses, comprising: providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; ... wherein said antivirus unit accesses at least one of the segments without using file-based information of the particular operating system or of any host having access to said at least one segment,* as set forth in Claim 1. Wells discloses detecting viruses by comparing data about a file to relational signature objects created from viruses. Wells' virus scanning is performed on a file-by-file basis and thus must use some file-based information. However, Wells appears silent regarding any further mention about the file-based information used in virus scanning. Frisch discloses dividing a disk into partitions each holding its own file system but fails to make any mention regarding what information is used in connection with accessing a segment during virus scanning. Kim operates on files and appears to use some file-based information. However, Kim appears silent regarding any further mention about the file-based information used in virus scanning.

Based on Applicant's understanding, Page 4 of the Office Action states that the prior art combination of Wells, Frisch and Kim teaches *wherein said antivirus unit accesses at least one of the segments without using file-based information ... of any host having access to said at*

Page 18 of 23

EMS-00201(2004734-0001)

least one segment, as set forth in Claim 1, in that the combination suggests using file-based

information of the particular operating system used by the antivirus unit in connection with

scanning for viruses. Thus, for at least this reason, Applicant respectfully submits that references

do not disclose or suggest Applicant's amended Claim 1 which explicitly recites that the

antivirus unit accesses at least one of the segments *without using file-based information of the*

particular operating system.

For reasons similar to those set forth regarding Claim 1, Claim 22 is also neither

disclosed nor suggested by the references in that the references neither disclose nor suggest *a*

method of scanning a storage device for viruses, comprising: ... wherein, when performing a

virus scan accessing at least one part of the storage device that is also accessible to at least

one host, said accessing of said at least one part is performed without using file-based

information of the particular operating system or of any host having access to said at least one

part, as set forth in Claim 22.

For reasons similar to those set forth regarding Claim 1, Claim 26 is also neither

disclosed nor suggested by the references in that the references neither disclose nor suggest *a*

computer program product for detecting computer viruses, comprising: means for accessing a

disk space having at least a portion that is partitioned into separate segments, each segment

being accessed by at least one of a plurality of hosts, wherein a first one of the segments is

accessed using a different file system than a second one of the segments; ... wherein, when

performing a virus scan accessing at least one of the segments that is also accessible to at least

one of said plurality of hosts, said accessing of said at least one segment is performed without

using file-based information of the particular operating system or of any host having access to
said at least one segment, as set forth in Claim 26.

For reasons similar to those set forth regarding Claim 1, Claim 36 is also neither disclosed nor suggested by the references in that the references neither disclose nor suggest *a computer program product for scanning a storage device for viruses, comprising: means for performing a first virus scan at a first time; ... .wherein, when performing a virus scan accessing at least one part of the storage device that is also accessible to at least one host, said accessing of said at least one part is performed without using file-based information of the particular operating system or of any host having access to said at least one part,* as set forth in Claim 36.

For reasons similar to those set forth regarding Claim 1, Claim 39 is also neither disclosed nor suggested by the references in that the references neither disclose nor suggest *an antivirus scanning unit, comprising: means for coupling to at least one storage device having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; ... wherein, when performing a virus scan accessing at least one of the segments that is also accessible to at least one of said plurality of hosts, said accessing of the at least one segment is performed without using file-based information of the particular operating system or of any host having access to said at least one segment,* as set forth in Claim 39.

For reasons similar to those set forth regarding Claim 1, Claim 47 is also neither disclosed nor suggested by the references in that the references neither disclose nor suggest Claim 47, as amended herein, recites *an antivirus unit, comprising: means for performing a first virus scan at a first time; and means for performing a second virus scan at a second time after the first time, ... wherein, when performing a virus scan accessing at least one part of the storage device that is also accessible to at least one host, said accessing of said at least one part is performed without using file-based information of the particular operating system or of any host having access to said at least one part*, as set forth in Claim 47.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

The rejection of Claim 43 under 35 U.S.C. § 103(a) as being unpatentable over Wells in view of Frisch and Kim and further in view of U.S. Patent No. 6,088,803 to Tso, et al. (hereinafter "Tso") is hereby traversed and reconsideration thereof is respectively requested in view of amendments to claims contained herein.

Claim 43 depends from independent Claim 39. For reasons set forth above, Wells, Frisch and Kim neither disclose nor suggest Claim 39. For reasons set forth below, combining Wells, Frisch and Kim with Tso also neither discloses nor suggests Claim 39, and claims that depend therefrom.

Wells, Frisch, and Kim are also discussed above.

As set forth on pages 15-16 of the Office Action, Tso discloses an antivirus accelerator for computer networks wherein an antivirus unit is interposed between a storage device and a host.
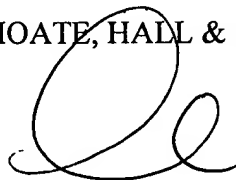
Applicants respectfully submit that combining Tso with the references of Wells, Frisch and Kim does not overcome the deficiencies of Wells, Frisch, and Kim with respect to Applicant's amended Claim 39, as discussed above, from which Claim 43 ultimately depends.

In view of the foregoing, Applicants respectfully request that this rejection be reconsidered and withdrawn. Applicant respectfully submits that newly added Claims 51-54 are also patentable over the cited art.

Based on the above, Applicant respectfully requests that the Examiner reconsider and withdraw all outstanding rejections and objections. Favorable consideration and allowance are earnestly solicited. Should there be any questions after reviewing this paper, the Examiner is invited to contact the undersigned at 617-248-4042.

Respectfully submitted,

CHOATE, HALL & STEWART LLP

Anne E. Saturnelli
Registration No. 41,290

Patent Group
CHOATE, HALL & STEWART LLP
Two International Place
Boston, MA 02110
Tel: (617) 248-5000
Fax: (617) 248-4000

Date: <u>August 26, 2005</u>